Symantec AntiVirus™ Corporate Edition Client Guide

Symantec AntiVirus™ Corporate Edition Client Guide

Documentation version 9.0

Copyright Notice

Trademarks

Printed in the United States of America.
10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/ function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support Program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to www.symantec.com/techsupp/ent/enterprise.html, select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at www.symantec.com/techsupp.

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
  - Error messages/log files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com, select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1

Introducing Symantec AntiVirus

This chapter includes the following topics:

About Symantec AntiVirus

Your Symantec AntiVirus virus protection may be installed as either a stand-alone or an administrator-managed installation. A stand-alone installation means that your Symantec AntiVirus software is not managed by a network antivirus administrator.

If you manage your own computer, it must be one of the following types:

- A stand-alone computer that is not connected to a network, such as a home computer or a laptop stand-alone, with a Symantec AntiVirus installation that uses either the default option settings or administrator-preset options settings
- A remote computer that connects to your corporate network that must meet security requirements before connecting

The default settings for Symantec AntiVirus provide complete virus protection for your computer. However, you may want to adjust them to optimize system

performance, to disable options that do not apply, and to allow Symantec AntiVirus to scan for threats other than viruses, such as adware and spyware.

If your installation is managed by your antivirus administrator, some options may be locked or unavailable, or may not appear at all, depending upon your administrator's antivirus policy. Your administrator runs scans on your computer and can set up scheduled scans.

Your antivirus administrator will advise you as to what tasks you should perform using Symantec AntiVirus.

Note: Options that display a padlock icon are not available because they have been locked by your antivirus administrator. You cannot change these options unless the antivirus administrator unlocks them.

About remote computers that connect to a corporate network

Remote computers that connect to a corporate network can receive virus definitions files and program file updates and can be managed by the Symantec System Center administrator program.

System administrators may require remote computers that connect to a corporate network to meet some security requirements. For example, the computer may have to run Symantec AntiVirus with the most up-to-date virus definitions files before it can connect to the network. The computer may be denied access to the network until it meets the security requirements.

About viruses and other threats

A *virus* is a computer program that attaches a copy of itself to another computer program or document when it runs. Whenever the infected program runs or a user opens a document containing a macro virus, the attached virus program activates and attaches itself to other programs and documents.

Viruses generally deliver a payload, such as displaying a message on a particular date. Some viruses specifically damage data by corrupting programs, deleting files, or reformatting disks.

A *worm* is a special type of virus that replicates itself from one computer to another and can use memory. Worms generally exist inside other files, such as Microsoft Word or Excel documents. A worm may release a document that already has the worm macro inside of it.

A blended threat uses multiple methods and techniques to propagate and attack. For example, Nimda, a worm that infected over 2 million computers in a 24-hour

period, had both virus and worm characteristics, and propagated itself using four different infection methods.

In the context of Symantec AntiVirus, the term virus is used to cover all threats that work in a virus-like manner.

Other known programs, such as adware or spyware, may or may not be threats to a computer. Symantec AntiVirus can detect these other threat categories.

About other threat categories

Threats other than viruses are classified by the behavior in which they engage and the purpose for which they appear to be designed. Symantec AntiVirus can detect the following expanded threat categories:

- *Spyware*: Stand-alone programs that can secretly monitor system activity and detect information like passwords and other confidential information and relay the information back to another computer.
- *Adware*: Stand-alone or appended programs that secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content.

  Spyware and adware can be unknowingly downloaded from Web sites (typically in shareware or freeware), email messages, and instant messenger software. You may unknowingly download adware by accepting an End User License Agreement from a software program.
- *Dialers*: Programs that use a computer, without your permission or knowledge, to dial out through the Internet to a 900 number or FTP site, typically to accrue charges.
- *Joke programs*: Programs that can alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from Web sites (typically in shareware or freeware), email messages, or instant messenger software. It can then move the trash can away from the mouse when you attempt to delete or cause the mouse to click in reverse.
- *Remote access*: Programs that allow access over the Internet from another computer to gain information or to attack or alter your computer. For example, you may install a program, or it may be installed as part of some other process without your knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.
- *Hack tools*: Programs that are used by a hacker to gain unauthorized access to your computer. For example, one hack tool is a keystroke logger, which

tracks and records individual keystrokes and can send this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hack tools may also be used to create tools for virus creation.

- *Trackware*: Stand-alone or appended applications that trace a user's path on the Internet and send information to a target system. For example, the application can be downloaded from Web sites, email messages, or instant messenger software. It can then obtain confidential information regarding user behavior.
- *Security risks*: Threats that do not conform to the strict definitions of viruses, Trojan horses, worms, or other expanded threat categories, but which may present a threat to your computer and its data.

Symantec AntiVirus scans for viruses, Trojan horses, and worms by default. You must enable expanded threat scanning for Symantec AntiVirus to detect other types of threats.

The Symantec Security Response Web site provides the latest information about threats and contains extensive threat reference information, such as white papers and detailed information about viruses and other threats.

Figure 1-1 shows information about a hack tool threat and how Symantec Security Response suggests that you handle it.

Figure 1-1 Symantec Security Response expanded threat description

See "Accessing the Symantec Security Response Web site" on page 29.

How Symantec AntiVirus responds to viruses and other threats

Symantec AntiVirus safeguards computers from viruses and other threats no matter what the source. Computers are protected from viruses that spread from hard drives and floppy disks, and others that travel across networks. Computers are also protected from viruses and other threats that spread through email attachments or some other means. For example, a threat may install itself on your computer without your knowledge when you access the Internet.

Files within compressed files are scanned and cleaned. No separate programs or options changes are necessary for Internet-borne viruses. Auto-Protect scans uncompressed program and document files automatically as they are downloaded.

Symantec AntiVirus responds to virus-infected files with actions and backup actions. When a virus is detected during a scan, Symantec AntiVirus, by default, attempts to clean the virus from the infected file. If the file is cleaned, the virus is successfully and completely removed from the file. If for some reason Symantec AntiVirus cannot clean the file, Symantec AntiVirus attempts the backup action, moving the infected file to the Quarantine so that the virus cannot spread.

When your virus protection is updated, Symantec AntiVirus automatically checks to see if any files are stored in the Quarantine and gives you the option of scanning them using the new protection information.

Note: Your antivirus administrator may choose to scan files in the Quarantine automatically.

Symantec AntiVirus can respond to some other threat categories with deleting as the action and logging only as the backup action. Some threats cannot be deleted without causing another program on your computer, such as a Web browser, to fail. For these threat types, Symantec AntiVirus uses the log only action.

When Symantec AntiVirus discovers a threat other than a virus, it presents a link to Symantec Security Response, where you can learn the best way to handle the threat. Your system administrator may also send a customized message telling you how to respond.

How Symantec AntiVirus protects your computer

Virus infections can be easily avoided. Viruses that are quickly detected and removed from your computer cannot spread to other files and cause damage. When a virus is detected, Symantec AntiVirus notifies you that one or more of your files is infected.

Symantec AntiVirus provides these types of protection:

- Auto-Protect: Constantly monitors activity on your computer by looking for viruses when a file is executed or opened, and when modifications have been made to a file, such as renaming, saving, moving, or copying a file to and from folders. Auto-Protect does not look for threats in the expanded threats category.

- Signature-based scanning: Searches for residual virus signatures in infected files. This search is called a *scan*. Depending on how your computer is managed, you and your company's antivirus administrator can initiate signature-based or pattern-based scans to systematically check the files on your computer for viruses and other threats, such as adware or spyware. Scans can be run on demand, scheduled to run unattended, or run automatically at system startup. Signature-based scanning looks for threats in the expanded threats category during manual and scheduled scans.
- Advanced heuristics: Analyzes a program's structure, its behavior, and other attributes for virus-like characteristics. In many cases it can protect against threats (such as mass-mailing worms and macro viruses), if you encounter the threat before updating your virus definitions. Advanced heuristics looks for script-based threats in HTML, VBScript, and JavaScript files.

What keeps Symantec AntiVirus protection current

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. They also track new types of other threats, such as adware and spyware. Once a virus or other threat is identified, a *signature* (information about the virus or threat) is stored in a *virus definitions file*, which contains the necessary information to detect and eliminate the virus or other threat. When Symantec AntiVirus scans for viruses and other threats, it is searching for these types of signatures.

Symantec makes updated definitions available on an ongoing basis. Definitions are updated daily on the Symantec Security Response Web site. New definitions are made available at least weekly for delivery using LiveUpdate, and whenever a destructive new virus appears.

When new viruses are so complex that issuing new virus definitions files for them isn't sufficient, Symantec engineers can update the AntiVirus Engine with the latest virus detection and repair components. When necessary, AntiVirus Engine updates are included with the virus definitions files.

About the role of Symantec Security Response

The strength behind Symantec AntiVirus is Symantec Security Response. The increasing number of computer viruses and other threats requires effort to track, identify, and analyze new viruses and threats, and to develop new technologies to protect your computer.

Symantec Security Response researchers disassemble each virus sample to discover its identifying features and behavior. With this information, they

develop a virus definition that Symantec products use to detect and eliminate the new virus during scans.

Because of the speed at which new viruses spread, particularly over the Internet, Symantec Security Response has developed automated software analysis tools. With direct submissions over the Internet of infected files from your Central Quarantine to Symantec Security Response, the time from discovery to analysis, to return cure by email is shrinking from days to hours, and in the near future, to minutes.

Symantec Security Response researchers also research and produce technologies to protect computers from other threats, such as spyware, adware, and hack tools.

Symantec Security Response maintains an encyclopedia that provides detailed information about viruses and other threats. In necessary cases, they provide information about removing or uninstalling the threat. The encyclopedia is located on the Symantec Security Response Web site.

See "Accessing the Symantec Security Response Web site" on page 29.

How virus protection is updated

Your antivirus administrator determines how your virus definitions are updated. You may not have to do anything to receive new virus definitions.

The LiveUpdate feature in Symantec AntiVirus can be set up by your antivirus administrator to make sure that your virus and other threat protection remains current. With LiveUpdate, Symantec AntiVirus connects automatically to a special Web site, determines if your files need updating, downloads the proper files, and installs them in the proper location.

See "Keeping virus protection current" on page 25.

Chapter 2

Symantec AntiVirus basics

This chapter includes the following topics:

Opening Symantec AntiVirus

You can open Symantec AntiVirus in several ways.

To open Symantec AntiVirus

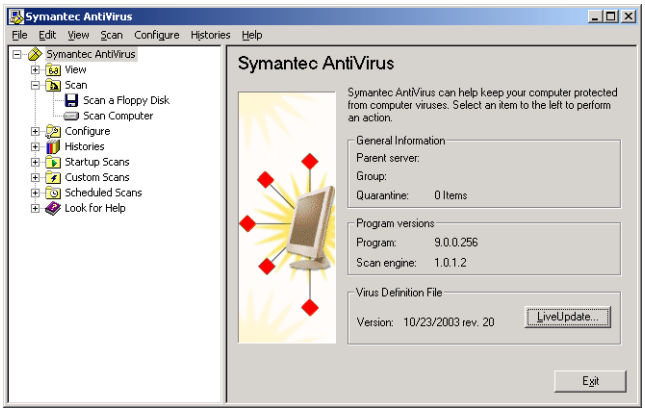
- Do one of the following:
  - On the Windows taskbar, double-click the Symantec AntiVirus icon.

    Your antivirus administrator determines whether this icon appears on the taskbar.
  - On the Windows taskbar, click **Start** > **Programs** > **Symantec Client Security** > **Symantec AntiVirus**.
  - On the Windows XP taskbar, click **Start** > **More Programs** > **Symantec Client Security** > **Symantec AntiVirus**.

Navigating in the Symantec AntiVirus main window

The Symantec AntiVirus main window is divided into two panes. The left pane groups activities that you can perform into categories. For example, Scan a Floppy Disk and Scan Computer are tasks in the Scan category. Individual icons represent each category in the left pane. When you select categories and other items in the left pane, the right pane displays the information that you need to perform a task.



To navigate in the Symantec AntiVirus main window

- In the left pane, do any of the following
  - Click a plus sign to expand a folder.
  - Click a minus sign to collapse a folder.
  - Select an item to access the information in the right pane.

Viewing Symantec AntiVirus categories

The activities that you can perform using Symantec AntiVirus are organized into seven main categories. Each category has a number of options that you can set.

The following tables do not discuss the individual options that you can change, but give a general description of what they do and how you can find them. For specific information about an option, see the online Help.

View category

You can use the View category to keep track of antivirus activities.

Table 2-1 View category

Option	Description
Auto-Protect Scan Statistics	View statistics about the status of Auto-Protect scans, including the last file that was scanned (even if it wasn't infected).
Scheduled Scans	View the list of all scheduled scans created to run on your computer, including the name of the scan, when it is scheduled to run, and who created it. A scheduled scan may be created by your company's antivirus administrator or by you.
Quarantine	Manage virus-infected files that have been isolated to prevent their spread. Symantec AntiVirus only moves virus-infected files to the Quarantine directory. It does not move other threats, such as spyware and adware. See "Rescanning files in the Quarantine" on page 45.
Backup Items	Delete backup copies of infected files. As a data safety precaution, Symantec AntiVirus makes a backup copy of infected items before attempting a repair. After verifying that Symantec AntiVirus cleaned an infected item of viruses, you should delete the copy in Backup Items. Symantec AntiVirus only backs up virus-infected files. It does not back up other threats, such as spyware and adware. See "Clearing Backup Items" on page 47.
Repaired Items	Release items that have been cleaned of viruses whose original locations are not known. For example, an infected attachment may have been stripped from an email message and quarantined. After the item is cleaned in the Quarantine and moved to Repaired Items, you must restore the item from Repaired Items and specify the location to which to restore it.
License	View information about the current license. Current license information includes the license status, serial number, and start and expiration dates. You can start the license installation wizard.

Scan category

You can use the Scan category to perform a manual scan of your computer.

Table 2-2 Scan category

Option	Description
Scan a Floppy Disk	Scan floppy disks and other removable media.
Scan Computer	Scan a file, folder, drive, or entire computer at any time. See "Initiating manual scans" on page 35.

Configure category

You can use the Configure category to set up Auto-Protect to monitor your files and email attachments (for supported email clients).

Table 2-3 Configure category

Option	Description
Auto-Protect	Whenever you access, copy, save, move, or open a file, it is examined to ensure that it is not infected. Auto-Protect includes the SmartScan feature which, when enabled, can determine a file's type even when a virus changes the file's extension. See "About Auto-Protect" on page 33.
Lotus Notes Auto-Protect and Microsoft Exchange Auto-Protect	For groupware email clients (Lotus Notes and Microsoft Exchange/Microsoft Outlook clients), Symantec AntiVirus includes additional protection for email.

Histories category

You can use the Histories category to track information about scans run on your computer and virus infections that are found.

Table 2-4 Histories category

Option	Description
Threat History	View a list of the viruses that have infected your computer with additional relevant information about the infection. View information about other threats, such as adware and spyware, that are installed on your computer. History for other threats includes a link to the Symantec Security Response Web page that describes the threat and provides handling instructions.
Scan History	Keep track of the scans that have occurred on your computer over time. Scans are displayed with additional relevant information about the scans.
Event Log	View a log of virus protection-related activities on your computer, including configuration changes, errors, and virus definitions file information.

Startup Scans category

You can use the Startup Scans category to create and configure scans to run when you start your computer.

Table 2-5 Startup Scans category

Option	Description
New Startup Scan	Some users supplement a scheduled scan with an automatic scan whenever they start their computers. Often, a startup scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Microsoft Word and Excel templates. See "Configuring startup scans" on page 38.

Custom Scans category

You can use the Custom Scans category to create preconfigured scans that you can run manually.

Table 2-6 Custom Scans category

Option	Description
New Custom Scan	If you regularly scan the same set of files or folders, you can create a custom scan restricted to those items. At any time, you can quickly verify that the specified files and folders are virus-free. See "Configuring custom scans" on page 39.

Scheduled Scans category

You can use the Scheduled Scans category to create preconfigured scans that run automatically at the times that you specify.

Table 2-7 Scheduled Scans category

Option	Description
New Scheduled Scan	Schedule a scan of your hard disks that runs at least once a week. A scheduled scan confirms that your computer remains virus-free. See "Creating scheduled scans" on page 37.

Enabling and disabling Auto-Protect

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses. It checks programs for viruses as they are run and monitors your computer for any activity that might indicate the presence of a virus. When a virus or *virus-like activity* (an event that could be the work of a virus) is detected, Auto-Protect alerts you.

In some cases, Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. For example, this might occur when you are installing new computer programs. If you will be performing such an activity and want to avoid the warning, you can temporarily disable Auto-Protect. Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

Your administrator might lock Auto-Protect so that you cannot disable it for any reason, or specify that File Auto-Protect can be disabled temporarily, but reenables automatically after a specified amount of time.

Enable and disable Auto-Protect

The Symantec AntiVirus icon is displayed on the taskbar in the lower-right corner of your Windows desktop. In some configurations, the icon is not displayed.

The Symantec AntiVirus icon appears as a full shield and a check mark appears next to Enable Auto-Protect when Auto-Protect is enabled.

The Symantec AntiVirus icon is covered by a universal no sign (a red circle with a diagonal slash) when Auto-Protect is disabled.

To enable and disable Auto-Protect from the taskbar

- On the Windows desktop, in the system tray, right-click the Symantec AntiVirus icon, and then click **Enable Auto-Protect**.

To enable and disable Auto-Protect from Symantec AntiVirus

1. In Symantec AntiVirus, in the left pane, click **Configure**.
2. In the right pane, click **Auto-Protect**.
3. Check or uncheck **Enable Auto-Protect**.
4. Click **OK**.
   The current Auto-Protect status updates dynamically to the right of the check box.

Pausing and delaying scans

The Pause feature lets you stop a scan at any point during the scan and resume it at another time. You can pause any scan that you initiate. Your network antivirus administrator determines whether you can pause an administrator-scheduled scan.

For scheduled scans that your network antivirus administrator initiates, you may also be allowed to delay the scan. If your administrator has enabled the Snooze feature, you can delay an administrator-scheduled scan for a set interval of time. When the scan resumes, it restarts from the beginning.

Pause the scan if you're planning on resuming it after a temporary break. Use the Snooze feature to delay the scan for a longer period of time during which you don't want to be interrupted, for example, if you're in the middle of a presentation.

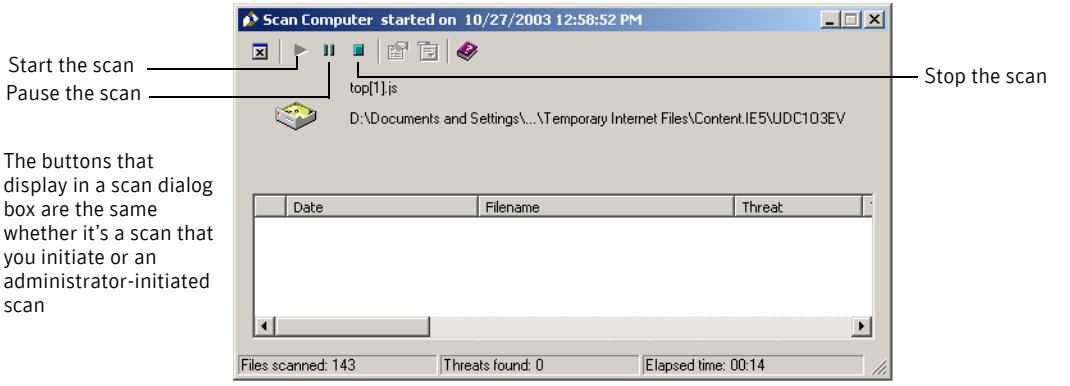
Pause or delay a scan

Use the following procedures to pause a scan initiated by you or delay an administrator-scheduled scan. If the Pause the Scan button is not available, your network antivirus administrator has disabled the Pause feature.

Note: If Symantec AntiVirus is scanning a compressed file when you choose to pause a scan, it may take several minutes to respond.

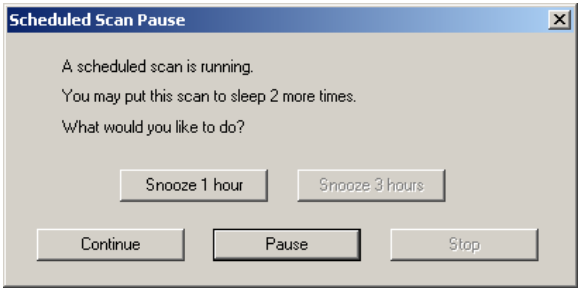
To pause a scan

1 When the scan runs, in the Scan Computer dialog box, click the pause icon.



The buttons that display in a scan dialog box are the same whether it's a scan that you initiate or an administrator-initiated scan

If it's a scan that you initiated, the scan stops where it is and the scan dialog box remains open until you start the scan again.
If it's an administrator-scheduled scan, the Scheduled Scan Pause dialog box appears.



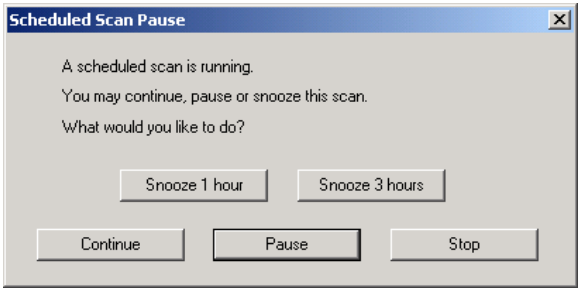
2 In the Scheduled Scan Pause dialog box, click **Pause**.
The administrator-scheduled scan stops where it is and the scan dialog box remains open until you start the scan again.

3 In the scan dialog box, click the start icon to continue the scan.

To delay an administrator-scheduled scan

1 When the administrator-scheduled scan runs, in the scan dialog box, click **Pause the Scan**.

2 In the Scheduled Scan Pause dialog box, click **Snooze 1 hour** or **Snooze 3 hours**.



Your administrator specifies the period of time that you're allowed to delay the scan. When you've reached that set period of time, the scan restarts from the beginning. Your administrator specifies the number of times that you can delay the scheduled scan before this feature is disabled.

Keeping virus protection current

Symantec AntiVirus relies on up-to-date information to detect and eliminate viruses. One of the most common reasons that virus problems occur is that virus definitions files are not updated after installation. The virus definitions files contain the necessary information about all newly discovered viruses.

Symantec supplies updated virus definitions files weekly through LiveUpdate and daily through Intelligent Updater files posted to the Symantec Security Response Web site. (Updates are also issued whenever a new high-risk virus threat emerges.) Make it a practice to update virus definitions once a week at a minimum. Scheduling LiveUpdate to run automatically is the easiest way not to forget. Always update immediately if a new virus scare is reported.

With LiveUpdate, Symantec AntiVirus connects automatically to a special Symantec Web site and determines if virus definitions need updating. If so, it downloads the proper files and installs them in the proper location. LiveUpdate also checks for and downloads program patches to Symantec AntiVirus, if available. Generally, you do not have to do anything to configure LiveUpdate. The only requirement is an Internet connection.

Note: Your administrator may have specified a maximum number of days that the virus definitions can be out-of-date. After exceeding the maximum number of days, Symantec AntiVirus automatically runs LiveUpdate when an Internet connection is detected.

Scheduling virus protection updates with LiveUpdate

By default LiveUpdate is scheduled to run automatically every Friday at 8 p.m. When the scheduled update runs, your computer must be running and have access to the Internet.

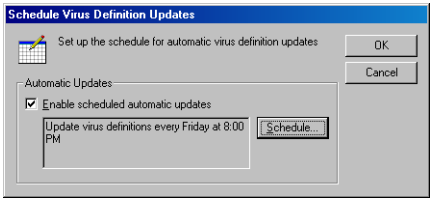
Schedule virus protection updates with LiveUpdate

You can change the LiveUpdate frequency and time to fit your needs.

Note: In a centrally managed network, your administrator may roll out updated virus definitions to workstations. In this case, you do not have to do anything.

To enable scheduled LiveUpdate

1 In Symantec AntiVirus, on the File menu, click **Schedule Updates**.



2 In the Schedule Virus Definition Updates dialog box, check **Enable scheduled automatic updates**.

3 Click **OK**.

4 In the Schedule Virus Definition Updates dialog box, click **OK**.

To set LiveUpdate schedule options

1 In the Schedule Virus Definition Updates dialog box, click **Schedule**.

2 In the Virus Definition Update Schedule dialog box, specify the frequency, day, and time that you want LiveUpdate to run.

3 Click **OK**.

To set advanced LiveUpdate schedule options

1 In the Virus Definition Update Schedule dialog box, click **Advanced**.

2 In the Advanced Schedule Options dialog box, do any of the following:

- To set up Symantec AntiVirus so that scheduled LiveUpdate events that are missed run at a later time, check **Handle Missed Events Within** and set the days.
- To set up Symantec AntiVirus so that scheduled LiveUpdate events run within a specified time range rather than at a set time, check the type of randomization method that you want to use and set the minute, day of the week, or day of the month.

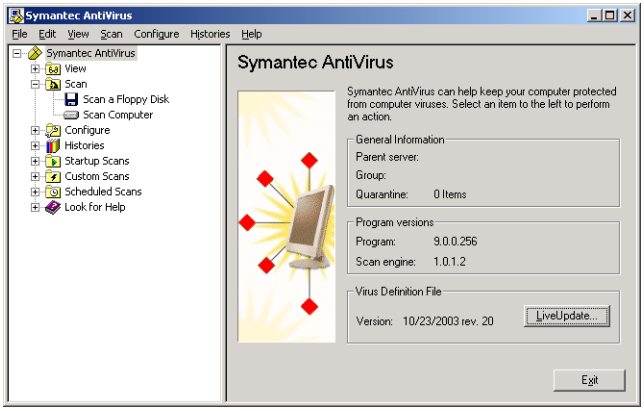
3 Click **OK**.

Updating virus protection immediately with LiveUpdate

When a new virus is reported, do not wait for your next scheduled update. You should update virus protection immediately.

To update virus protection immediately with LiveUpdate

1 In Symantec AntiVirus, in the left pane, click **Symantec AntiVirus**.



2 In the right pane, click **LiveUpdate**.

3 If necessary, in the left pane, click **Configure** to customize your Internet connection for LiveUpdate.
You can change your Internet service provider connection or how your computer connects through a proxy server to the Internet.
For more information, use the online Help from LiveUpdate.

4 Click **Next** to start the automatic update.

Updating without LiveUpdate

Symantec supplies a special program called Intelligent Updater as an alternative to LiveUpdate. You can download the updates from the Symantec Security Response Web site.

See "Accessing the Symantec Security Response Web site" on page 29.

To update without LiveUpdate

1. Download the Intelligent Updater program to any folder on your computer.
2. In a My Computer or Windows Explorer window, locate and then double-click the Intelligent Updater program.
3. Follow all prompts displayed by the update program.
   The Intelligent Updater program searches your computer for Symantec AntiVirus, and then installs the new virus definitions files in the proper folder automatically.
4. Scan your disks to make sure that newly discovered viruses are detected.

For more information

If you need more information about Symantec AntiVirus, you can access the online Help. In addition, information about viruses can be obtained from the Symantec Web site.

Accessing online Help

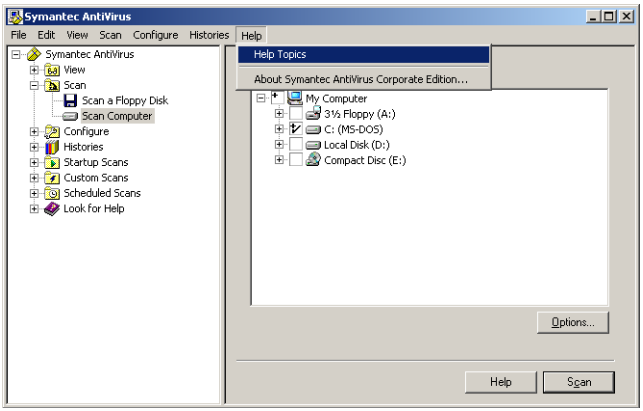
The Symantec AntiVirus online Help system has general information and step-by-step procedures to help you keep your computer safe from viruses.

Note: Your administrator may have elected not to install the Help files.

To get help using Symantec AntiVirus

- In Symantec AntiVirus, do one of the following:
  - On the Help menu, click **Help Topics**.
  - In the right pane, click **Help**.

Context-sensitive Help is available only in screens on which you can perform actions.



Accessing the Symantec Security Response Web site

If you are connected to the Internet, you can visit the Symantec Security Response Web site to view items such as the following:

- The Virus Encyclopedia, which contains information about all known viruses
- Information about virus hoaxes
- White papers about viruses and virus threats in general
- General and detailed information about expanded threats

To access the Symantec Security Response Web site

- In your Internet browser, type the following Web address: **securityresponse.symantec.com**

Chapter 3

Protecting your computer from viruses

This chapter includes the following topics:

About Symantec AntiVirus antivirus policy

Symantec AntiVirus comes preset with an antivirus policy that is appropriate for most users. You can change settings based on your personal needs. You can separately customize policy settings for Auto-Protect, manual, scheduled, startup, and custom scans.

An antivirus policy determines:

- What to scan
- What to do if a virus is detected

What to scan

Symantec AntiVirus Auto-Protect scans all file types by default. Manual, scheduled, startup, and custom scans also examine all file types by default.

Auto-Protect includes SmartScan, which scans files with the extensions included in the Program File Extensions List. SmartScan also scans all

executable files and Microsoft Office documents whether or not the extensions are listed in the Program File Extensions List.

See "Modifying Auto-Protect and using SmartScan" on page 34.

You can choose to scan files by file extension or by type of file (documents and programs), but your protection from viruses is reduced.

You can also choose to exclude specific files from scanning. For example, if a file that you know is not infected triggers a virus alert during a scan, you prevent further warnings by excluding the file from your subsequent scans.

Scan by file types or extensions

Symantec AntiVirus can scan your computer by file types or by extensions.

To select file types to scan

1. In Symantec AntiVirus, in the left pane, select the scan that you want to change.
   - If you selected an on-demand scan, click **Options**.
   - If you selected a startup, custom, or scheduled scan, click the name of the scan to change, and then click **Edit**.
     Changes will apply only to the specific scan that you select.
   - If you selected Auto-Protect, go to step 2.
2. Click **Selected**, and then click **Types**.
3. Select one or more of the following file types:
   - Document files: Include Word and Excel documents, and template files associated with those documents.
   - Program files: Include dynamic-link libraries (.dll), batch files (.bat), communication files (.com), executable files (.exe), and other program files.
4. For on-demand scans, if you want to permanently use these actions for all subsequent on-demand scans, click **Save Settings**.
5. Click **OK**.

What to do if a virus is detected

Symantec AntiVirus responds to infected files with actions and backup actions. By default, when a virus is detected by either Auto-Protect or during a scan, Symantec AntiVirus attempts to clean the virus from the infected file. If Symantec AntiVirus cannot clean the file, the backup action is to log the failed

cleaning attempt and move the infected file to the Quarantine so that the virus cannot spread, which denies you further access to the file.

Depending on your antivirus policy, you can change these settings to delete an infected file on detection or leave it alone (log only). For Auto-Protect, you can also choose to deny access. In addition, you can set different actions for macro and nonmacro viruses for each scan type separately.

About Auto-Protect

Auto-Protect is your best defense against virus attack. Whenever you access, copy, save, move, or open a file, Auto-Protect scans the file to ensure that a virus has not attached itself.

Auto-Protect includes SmartScan, which scans a group of file extensions that contain executable code and all .exe and .doc files. SmartScan can determine a file's type even when a virus changes the file's extension. For example, it scans .doc files even when a virus changes the file extension to one that is different from the file extensions that SmartScan has been configured to scan.

To supplement Auto-Protect, Symantec AntiVirus detects at installation whether you use a supported groupware email client and adds Auto-Protect for email. Protection is provided for the following email clients:

- Lotus Notes 4.5x, 4.6, 5.0, and 6.0
- Microsoft Exchange 5.0 and 5.5, Microsoft Outlook 97, Microsoft Outlook 98 (MAPI only, not Internet), Microsoft Outlook 2000, and Microsoft Outlook 2002

Symantec AntiVirus also includes Auto-Protect scanning for additional Internet email programs by monitoring all traffic that uses the POP3 or SMTP communications protocols. You can configure Symantec AntiVirus to scan incoming messages for threats as well as outgoing messages for known heuristics using Bloodhound Virus Detection. Scanning outgoing email helps to prevent the spread of threats such as worms that can use email clients to replicate and distribute themselves across a network.

For Lotus Notes and Microsoft Exchange email scanning, Symantec AntiVirus scans only the attachments that are associated with email. For Internet email scanning of messages that use the POP3 or SMTP protocols, Symantec AntiVirus scans both the body of the message and any attachments that are included.

When Auto-Protect is enabled for a supported email client and you open a message with an attachment, the attachment is immediately downloaded to your computer and scanned. Over a slow connection, downloading messages

with large attachments affects mail performance. You may want to disable this feature if you regularly receive large attachments.

There are times, such as during the installation of new software, that you must temporarily disable Auto-Protect.

See "Enabling and disabling Auto-Protect" on page 22.

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- POP3 that uses Secure Sockets Layer (SSL)
- Web-based email such as Hotmail and Yahoo!

Note: Email Auto-Protect works on your supported email client only. It does not protect email servers.

Modifying Auto-Protect and using SmartScan

Auto-Protect is preset to scan all files. Scanning all files or using SmartScan offers the most protection from viruses. SmartScan is enabled by default.

Symantec AntiVirus may complete scans faster by scanning only files with selected extensions, such as .exe, .com, .dll, .doc, and .xls. Although this method offers less protection, it is an efficient way to scan because viruses affect only certain file types. The default list of extensions represents those files that are commonly at risk of infection.

To modify Auto-Protect and use SmartScan

1. In Symantec AntiVirus, in the left pane, click **Configure**.
2. In the right pane, click **Auto-Protect**.
3. In the File Types group box, do one of the following:
   - Click **All Types** to instruct Symantec AntiVirus to scan all files.
   - Click **Selected** to instruct Symantec AntiVirus to scan only those files that match the listed file extensions, and then click **Extensions** to change the default list of file extensions.
   - Ensure that SmartScan is checked for Symantec AntiVirus to scan using this feature.
4. Click **OK** to save your settings.

Scanning for viruses

In addition to Auto-Protect, which is your most powerful defense against virus infection, Symantec AntiVirus supplies several different types of scans to provide additional protection. Scan types include the following:

- Manual scans: Scan a file, folder, drive, or entire computer at any time.
- Scheduled scans: Run unattended at a specified frequency.
- Startup scans: Run every time you start your computer and Windows loads.
- Custom scans: Scan specified file sets at any time.

A single, weekly scheduled scan of all files is generally sufficient protection, as long as Auto-Protect is always running. If your computer is frequently attacked by viruses, consider adding a startup scan or daily scheduled scan. Another good habit is to always scan floppy disks when first used, particularly if they have been circulating among users.

About scanning compressed and encoded files

Symantec AntiVirus scans within compressed and encoded files, for example, .zip files. Your administrator can specify scanning up to 10 levels deep for compressed files that contain compressed files. Check with your administrator for the types of compressed file scans that are supported.

If Auto-Protect is enabled, any file that is removed from a compressed file is scanned, thereby protecting your computer.

Initiating manual scans

You can manually scan for viruses and other threats, such as adware and spyware, at any time. Select anything from a single file to a floppy disk to your entire computer.

Initiate manual scans

You can initiate scans from the My Computer or Windows Explorer window or from the Symantec AntiVirus main window.

To initiate a manual scan from Windows

- In a My Computer or Windows Explorer window, right-click a file, folder, or drive, and then click **Scan For Viruses**.

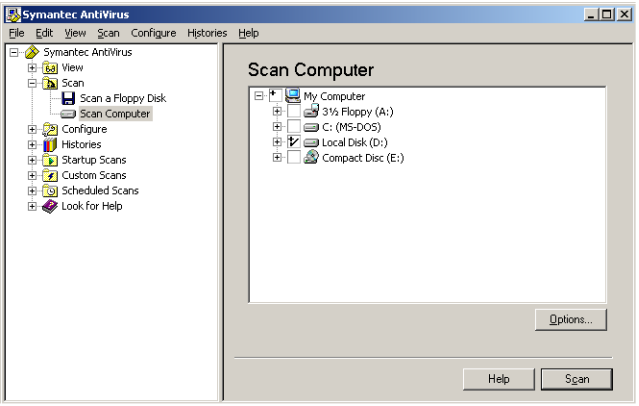
Note: This feature is not supported on 64-bit operating systems.

To initiate a manual scan within Symantec AntiVirus

1 In Symantec AntiVirus, in the left pane, expand **Scan**.

2 In the left pane, select one of the following:

- Scan a Floppy Disk
  This option is available only when a floppy disk drive is present.
- Scan Computer



3 In the right pane, do the following:

- Double-click a drive or folder to open or close it.
- Check or uncheck items that you want to scan.
  The symbols mean the following:

The file, drive, or folder is not selected. If the item is a drive or folder, the folders and files in it are also not selected.

The individual file or folder is selected.

The individual folder or drive is selected. All items within the folder or drive are also selected.

The individual folder or drive is not selected, but one or more items within the folder or drive are selected.

4 Click **Options** to change to the default settings for what is scanned and how to respond if a virus is detected.
The preset options are to scan all files, clean the virus from an infected file, and quarantine the infected file if the virus cannot be removed. Generally, it is only necessary to change settings for expanded threats and in-memory threat scanning. You must enable both of these options in the Scan Options dialog box.
To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.

5 Click **Scan**.
Symantec AntiVirus begins the scan and reports the results.

Creating scheduled scans

A scheduled scan is an important component of threat protection. At the very least, schedule a scan to run once a week to ensure that your computer remains free of viruses and other threats, such as adware and spyware.

Note: If your network antivirus administrator has created a scheduled scan for you, it appears in the Scheduled Scans area of the View folder, not in the Scheduled Scans folder. The Scheduled Scans folder only displays scans that you've scheduled.

To create a scheduled scan

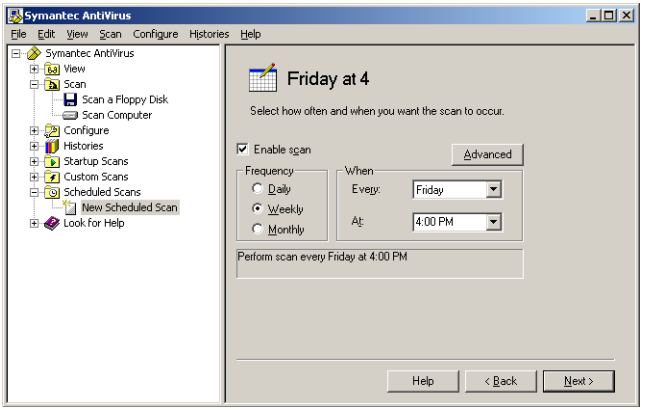
1 In Symantec AntiVirus, in the left pane, click **Scheduled Scans**.

2 In the right pane, click **New Scheduled Scan**.

3 Type a name and description for the scan.
For example, call the scan "Friday at 4."

4 Click **Next**.

5 Specify the frequency for the scan.



6 Click **Next**.

7 In the tree control, check boxes to specify where to scan.
You can check anything from the entire computer to a single file.
See "Initiating manual scans" on page 35.

8 Click **Options** to change to the default settings for what is scanned and how to respond if a virus is detected.
The preset options are to scan all files, clean the virus from an infected file, and quarantine the infected file if the virus cannot be removed. Generally, it is only necessary to change settings for expanded threats and in-memory threat scanning. You must enable both of these options in the Scan Options dialog box.
To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.

9 Click **Save**.
Your computer must be turned on and Symantec AntiVirus Services must be loaded when the scan is scheduled to take place. (By default, Symantec AntiVirus Services are loaded when you start your computer.)
The new scan is added to the list in the Scheduled Scans folder.

Configuring startup scans

Some users supplement a scheduled scan with an automatic scan whenever they start their computers. Often, a startup scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Microsoft Word and Excel templates.

Note: If you create more than one startup scan, the scans will run sequentially in the order in which they were created.

To configure a startup scan

1. In Symantec AntiVirus, in the left pane, click **Startup Scans**.
2. In the right pane, click **New Startup Scan**.
3. Type a name and description for the scan.
4. Click **Next**.
5. In the tree control, check boxes to specify where to scan.
   You can check anything from the entire computer to a single file.
   See "Initiating manual scans" on page 35.
6. Click **Options** to change to the default settings for what is scanned and how to respond if a virus is detected.
   The preset options are to scan all files, clean the virus from an infected file, and quarantine the infected file if the virus cannot be removed. Generally, it is only necessary to change settings for expanded threats and in-memory threat scanning. You must enable both of these options in the Scan Options dialog box.
   To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.
7. Click **Save**.
   The scan will run every time that you start your computer and Windows loads.

Configuring custom scans

If you regularly scan the same set of files or folders, you can create a custom scan restricted to just those items. At any time, you can quickly verify that the specified files and folders are free from viruses and other threats.

Configure custom scans

You can create a custom scan that can be run manually at any time.

To create a custom scan

1. In Symantec AntiVirus, in the left pane, click **Custom Scans**.
2. In the right pane, click **New Custom Scan**.
3. Type a name and description for the scan.

4 Click **Next**.

5 In the tree control, check boxes to specify where to scan.
You can check anything from the entire computer to a single file.
See "Initiating manual scans" on page 35.

6 Click **Options** to change to the default settings for what is scanned and how to respond if a virus is detected.
The preset options are to scan all files, clean the virus from an infected file, and quarantine the infected file if the virus cannot be removed. Generally, it is only necessary to change settings for expanded threats and in-memory threat scanning. You must enable both of these options in the Scan Options dialog box.
To apply the modified settings only to the current scan, click **OK**. To apply the settings to all future scans, click **Save Settings**.

7 Click **Save**.

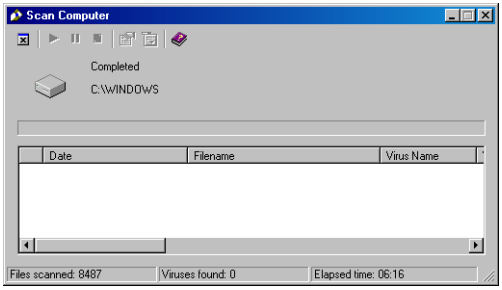
To run a custom scan

1 In Symantec AntiVirus, in the left pane, expand **Custom Scans**.

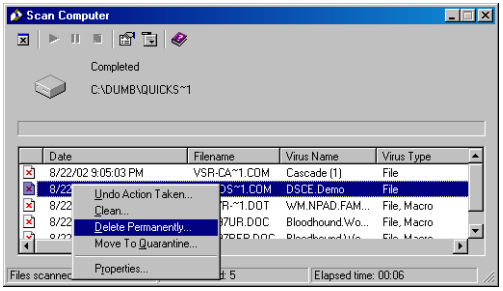
2 Double-click the saved custom scan.

Interpreting scan results

Whenever a manual, scheduled, startup, or custom scan runs, Symantec AntiVirus displays a Scan Computer dialog box to report progress. You can pause, restart, or stop the scan. At the completion of the scan, results are reported in the list box. If no viruses are detected, the list box is blank and the status is completed.



If viruses are detected during the scan, the dialog box includes the name of the infected file, the name of the virus, and the action taken. An alert is also generated, by default, whenever a virus is detected.



See "Acting on infected files" on page 43.

Note: In a centrally managed network, the Scan Computer dialog box may not appear for administrator-initiated scans. Similarly, your administrator may choose not to display alerts when a virus is detected.

Excluding files from scans

Rarely, a file that does not contain a virus is detected as infected. This might happen because a particular virus definition is designed to catch every possible variation of the virus. Because the virus definition must be necessarily broad, Symantec AntiVirus sometimes reports that a clean file is infected.

If Symantec AntiVirus continues to report a clean file as infected, you can exclude the file from scans. Exclusions are items that you don't want or need to include in scans.

You can also exclude folders if they contain software that can be detected as threats, such as trackware, and your corporate security policy allows you to run the software.

See "About other threat categories" on page 9.

Set exclusions separately for each type of scan: Auto-Protect, manual, scheduled, startup, or custom. The procedure, however, is the same.

Warning: Be careful with exclusions. If you exclude a file from a scan, no action will be taken to clean it if the file later becomes infected. This could be a potential risk to the security of your computer.

To exclude a file from a scan

1. In Symantec AntiVirus, do one of the following:
   - For Auto-Protect of the file system, in the left pane, click **Configure**, and then, in the right pane, click **Auto-Protect**.
   - For mail Auto-Protect of email attachments, in the left pane, click **Configure**, and then, in the right pane, click **Lotus Notes Auto-Protect** or **Microsoft Exchange Auto-Protect**.
   - For all other scan types, in the pane where you specify what to scan, click **Options**.
2. Check **Exclude Selected Files And Folders**.
3. Click **Exclusions** to specify the file to exclude, and then click **OK**.
4. To enable prescan exclusions, check **Check File For Exclusion Before Scanning**.
   Different situations determine how this option affects performance. For example:
   - If you copy a large folder that is in the exclusions list and prescan exclusions is enabled, the copying process is shorter since the folder contents are excluded prior to scanning.
   - If you copy a large folder that is not in the exclusions list, disabling prescan exclusions improves performance.
5. Click **Extensions**.
6. Specify the file types that you want to exclude.
   You can use the ? wildcard character to specify any character. For example, XL? excludes .xls, .xlt, .xlw, and .xla files.
7. Click **Files/Folders**.
8. Specify what to exclude.
9. Click **OK**.

Chapter 4

What to do if a virus or other threat is found

This chapter includes the following topics:

Acting on infected files

The Symantec AntiVirus preset options for Auto-Protect and all scan types are to clean a virus from an infected file on detection, but to place the file in the Quarantine if it cannot be cleaned.

If an infected file is repaired, you don't need to take further action to protect your computer.

You can deal immediately with infected files from the Scan Computer dialog box once a scan completes. For example, you may decide to delete a cleaned file because you'd rather replace it with an original file.

To deal with an infected file at a later point, you can do so from the Threat History or from the Quarantine.

See "Rescanning files in the Quarantine" on page 45.

Note: In a centrally managed network, the Scan Computer dialog box may not appear for administrator-initiated scans. Similarly, your administrator may choose not to display alerts when a virus is detected.

To act on an infected file

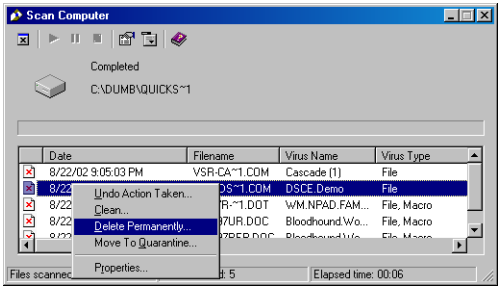
1 Do one of the following:

- In the Scan Computer dialog box, select the files that you want once the scan completes.
- In Symantec AntiVirus, in the left pane, expand **Histories**, click **Threat History**, and then, in the right pane, select the files you want.

2 Right-click the file or files, and then select one of the following:

- Undo Action Taken: If possible, reverses the preset action response
- Clean: Removes the virus from the file
- Delete Permanently: Deletes the infected file
- Move To Quarantine: Places the infected file in the Quarantine
- Properties: Displays information about the virus

Depending on the preset action for a virus detection, your selection may not be able to be performed.



Managing the Quarantine

Sometimes Symantec AntiVirus detects an unknown virus that can't be eliminated with the current set of virus definitions, or you have a file that you think is infected but is not being detected. The Quarantine safely isolates potentially infected files on your computer. A virus in a quarantined item cannot spread.

Files are placed in the Quarantine in one of two ways:

- Symantec AntiVirus is configured to move infected items detected during Auto-Protect or a scan to the Quarantine.
- You manually select a file and add it to the Quarantine.

The Symantec AntiVirus preset options for Auto-Protect and all scan types are to clean a virus from an infected file on detection, but to place the file in the Quarantine if it cannot be cleaned.

Note: Symantec AntiVirus does not place other threats, such as spyware and adware, in the Quarantine.

To add a file manually to the Quarantine

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Quarantine**.
3. On the toolbar, click **Add New Item to Quarantine**.
4. Locate the file, and then click **Add**.
5. Click **Close**.

Rescanning files in the Quarantine

If a file is placed in the Quarantine, update your virus definitions. Depending on how your administrator has configured the Quarantine, when virus definitions have been updated, files in the Quarantine might get scanned, cleaned, and restored automatically or the Repair Wizard might appear, letting you rescan the files in the Quarantine.

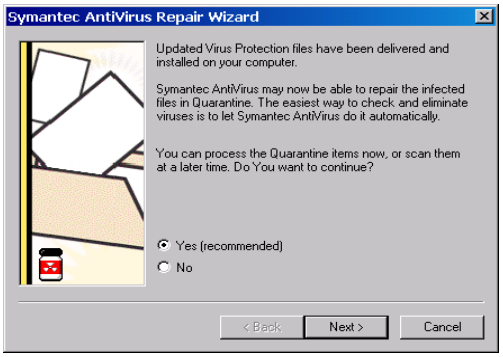
If after rescanning the file in the Quarantine, the virus still can't be removed, submit the infected file to Symantec Security Response for analysis. A new virus definitions file is developed to detect and clean the virus and the file is sent to you by email.

See "Submitting a potentially infected file to Symantec Security Response for analysis" on page 49.

To rescan files in the Quarantine using the Repair Wizard

1 If the Repair Wizard appears, click **Yes**.

2 Click **Next** and follow the on-screen instructions to rescan the files in the Quarantine.



Rescanning files manually

You can manually rescan a file in the Quarantine.

To rescan a file in the Quarantine manually

1 Update your virus definitions.
See "Keeping virus protection current" on page 25.

2 In Symantec AntiVirus, in the left pane, click **View**.

3 In the right pane, click **Quarantine**.

4 Select the file in the Quarantine listing.

5 Do one of the following:

- Right-click the file, and then click **Clean**.
- In the right pane on the toolbar, click **Clean**.

6 Click **Start Clean**.
The file is scanned again with the new definitions and replaced in its original location.

When a repaired file can't be returned to its original location

Occasionally, a clean file does not have a location to which to be returned. For example, an infected attachment may have been stripped from an email and placed in the Quarantine. In this special circumstance, the cleaned file is placed in Repaired Items instead. You must release the file and specify a location.

To release a cleaned file from Repaired Items

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Repaired Items**.
3. Right-click the file, and then click **Restore**.
4. Specify the location for the cleaned file.

Clearing Backup Items

As a data safety precaution, Symantec AntiVirus is configured to make a backup copy of an infected item before attempting a repair. After an infected item has been successfully cleaned, you should manually delete it from Backup Items because the backup is still infected. You can also set up a time period in which files are deleted automatically.

See "Automatically purging files from the Quarantine, Backup Items, and Repaired Items" on page 48.

Note: Symantec AntiVirus does not back up other threats, such as spyware and adware.

To manually clear Backup Items

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Backup Items**.
3. Select one or more files in the Backup Items listing.
4. Do one of the following:
   - Right-click the file, and then click **Delete Permanently**.
   - In the right pane on the toolbar, click **Delete**.
5. In the Take Action dialog box, click **Start Delete**.
6. Click **Close**.

Deleting files from the Quarantine

You can manually delete files that you no longer need from the Quarantine. You can also set up a time period by which files are deleted automatically.

See "Automatically purging files from the Quarantine, Backup Items, and Repaired Items" on page 48.

Note: Your administrator may specify a maximum number of days that items are allowed to stay in the Quarantine. Items are automatically deleted from the Quarantine after that time limit.

To manually delete files from the Quarantine

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, click **Quarantine**.
3. Select one or more files in the list of quarantined items.
4. Right-click the files, and then click **Delete Permanently**.
5. In the Take Action dialog box, click **Start Delete**.
6. Click **Close**.

Automatically purging files from the Quarantine, Backup Items, and Repaired Items

You can set up Symantec AntiVirus to automatically remove items after a specified time interval from the Quarantine, Backup Items, and Repaired Items. This prevents the buildup of files that you may forget to remove manually from these areas.

To automatically purge files

1. In Symantec AntiVirus, in the left pane, click **View**.
2. In the right pane, select one of the following:
   - Quarantine
   - Backup Items
   - Repaired Items
3. Click **Purge**.
4. In the Purge Options dialog box, check **Enable automatic files purging**.
5. In the Purge after text box, type a number or click an arrow to select a number.

6 Select the time period interval.

7 Click **OK**.

8 Click **Close**.

Submitting a potentially infected file to Symantec Security Response for analysis

Sometimes, Symantec AntiVirus cannot clean a virus from a file. Or, you suspect that a file is infected and is not being detected. Symantec Security Response analyzes your file to make sure that it is not infected. If a new virus is discovered in your submission, Symantec Security Response creates and sends you special updated virus definitions to detect and eliminate the new virus. You must have an Internet connection to submit a sample and an email address to receive a reply.

Note: In a centrally managed network, submissions to Symantec Security Response are usually handled by your antivirus administrator from the Symantec Central Quarantine. In this case, the Submit to Symantec Security Response option is not available in your version of Symantec AntiVirus. Also, the Submit to Symantec Security Response option is not available if the administrator configures an unmanaged client to not allow submissions to Symantec Security Response.

To submit a file to Symantec Security Response from the Quarantine

1 In Symantec AntiVirus, in the left pane, click **View**.

2 In the right pane, click **Quarantine**.

3 Select the file in the list of quarantined items.

4 In the right pane on the toolbar, click **Submit To Symantec Security Response**.

5 Follow the on-screen instructions in the wizard to collect the necessary information and submit the file for analysis.
You are notified by email with the results of the analysis, and, if appropriate, updated virus definitions.

Acting on threats in the Expanded Threats category

You must enable expanded threat detection before Symantec AntiVirus scans for certain threat types.

You can respond to other threats from the Scan Computer dialog box once the scan completes or from the Threat History.

To act on a threat in the Expanded Threats category

1. Do one of the following:
   - In the Scan Computer dialog box, double-click the file that you want once the scan completes.
   - In Symantec AntiVirus, in the left pane, expand **Histories**, click **Threat History**, and then, in the right pane, double-click the file that you want.
2. Read the information about the threat on the Symantec Security Response Web site, and then take the recommended action.
   See Figure 1-1, “Symantec Security Response expanded threat description,” on page 11.

Index